

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

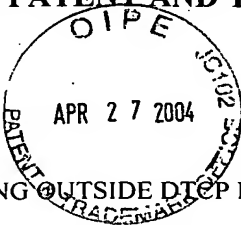
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takeshi SAITO, et al.

SERIAL NO: 10/722,515

FILED: November 28, 2003

FOR: COMMUNICATION SCHEME USING OUTSIDE DTEP BRIDGE FOR REALIZING COPYRIGHT PROTECTION



GAU:

EXAMINER:

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2002-344431	November 27, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak

Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26, 803

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 2 7 日
Date of Application:

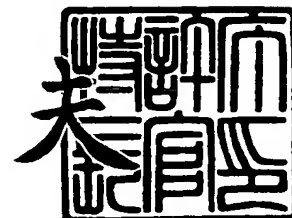
出 願 番 号 特 願 2 0 0 2 - 3 4 4 4 3 1
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 4 4 4 3 1]

出 願 人 株 式 会 社 東 芝
Applicant(s):

2 0 0 3 年 7 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 14002701

【提出日】 平成14年11月27日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明の名称】 通信中継装置、通信システム及び通信制御プログラム

【請求項の数】 13

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

【氏名】 斉 藤 健

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

【氏名】 磯 崎 宏

【特許出願人】

【識別番号】 000003078

【住所又は居所】 東京都港区芝浦一丁目 1 番 1 号

【氏名又は名称】 株式会社 東 芝

【代理人】

【識別番号】 100075812

【弁理士】

【氏名又は名称】 吉 武 賢 次

【選任した代理人】

【識別番号】 100088889

【弁理士】

【氏名又は名称】 橋 谷 英 俊

【選任した代理人】

【識別番号】 100082991

【弁理士】

【氏名又は名称】 佐 藤 泰 和

【選任した代理人】

【識別番号】 100096921

【弁理士】

【氏名又は名称】 吉 元 弘

【選任した代理人】

【識別番号】 100103263

【弁理士】

【氏名又は名称】 川 崎 康

【手数料の表示】

【予納台帳番号】 087654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信中継装置、通信システム及び通信制御プログラム

【特許請求の範囲】

【請求項 1】

宅外ネットワークに接続された宅外通信装置と、宅内ネットワークに接続された宅内通信装置との間で情報を中継する、前記宅内ネットワークに接続された通信中継装置であって、

前記宅内ネットワーク上の宅内通信装置との間での著作権保護のための第 1 の認証鍵交換処理を行う第 1 の著作権保護手段と、

前記宅外ネットワーク上の宅外通信装置との間での著作権保護のための前記第 1 の認証鍵交換処理とは異なる方式の第 2 の認証鍵交換処理を行う第 2 の著作権保護手段と、

前記宅外通信装置の識別情報を登録する識別情報記憶手段と、

前記宅外通信装置から接続要求があった場合には、

前記宅内ネットワークに接続要求を行った前記宅外通信装置が前記識別情報記憶手段に登録されていることを確認し、かつ前記接続要求についての前記第 1 及び第 2 の著作権保護手段による認証鍵交換が成功した場合に限り、前記宅内ネットワーク及び前記宅外ネットワークの間での情報の送受信を行うブリッジ処理手段と、を備えることを特徴とする通信中継装置。

【請求項 2】

前記識別情報記憶手段に登録可能な前記宅外通信装置の台数を所定数に制限し、いったん登録した識別情報の削除を禁止する登録制御手段を備えることを特徴とする請求項 1 に記載の通信中継装置。

【請求項 3】

前記識別情報記憶手段は、前記宅外通信装置にコンテンツを送信する前に予め前記著作権保護のために前記宅外通信装置を識別するデバイス ID と通信インタフェースの物理アドレスとの少なくとも一方を登録しておくことを特徴とする請求項 1 または 2 に記載の通信中継装置。

【請求項 4】

前記識別情報記憶手段は、前記宅外通信装置を前記宅内ネットワークに接続許可した状態で、前記第2の著作権保護手段による認証鍵交換処理を行った結果を登録するモードを持つことを特徴とする請求項1または2に記載の通信中継装置。

【請求項5】

前記宅外通信装置のユーザ認証情報を登録するユーザ情報記憶手段と、
前記宅内ネットワークに接続要求を行った前記宅外通信装置のユーザ認証情報が前記ユーザ情報記憶手段に登録されているか否かを判定する認証判定手段と、
を備え、

前記ブリッジ処理手段は、前記認証判定手段の判定結果に基づいて、前記宅内ネットワーク及び前記宅外ネットワークの間で接続を許可するか否かを判断することを特徴とする請求項4に記載の通信中継装置。

【請求項6】

前記宅外通信装置のユーザ認証情報を登録するユーザ情報記憶手段と、
前記宅内ネットワークに接続要求を行った前記宅外通信装置のユーザ認証情報が前記ユーザ情報記憶手段に登録されているか否かを判定する認証判定手段と、
を備え、

前記識別情報記憶手段は、前記認証判定手段の判定結果に基づいて、前記著作権保護のために前記宅外通信装置を識別するデバイスIDと通信インタフェースの物理アドレスとの少なくとも一方を登録することを特徴とする請求項4に記載の通信中継装置。

【請求項7】

前記宅内通信装置の制御または監視を行うための情報を記述したWebページを作成するWebページ作成手段と、

前記作成されたWebページを前記宅外ネットワークに送信するWebページ公開手段と、を備え、

前記宅外通信装置は、前記宅外ネットワークを介して受信した前記Webページを用いて前記宅内通信装置の制御または監視を行うことを特徴とする請求項1乃至6のいずれかに記載の通信中継装置。

【請求項 8】

前記第 1 の著作権保護手段は、前記宅内通信装置と前記宅外通信装置との間で送受されるパケットの TTL (Time To Live) フィールドを特定の値に制限すること、インターネットプロトコルとしてリンクローカルアドレスを使用すること、及び伝送パケットとしてイーサネット（登録商標）フレームを使用することの少なくとも一つを採用して著作権保護を図ることを特徴とする請求項 1 または 2 に記載の通信中継装置。

【請求項 9】

前記宅内ネットワーク及び前記宅外ネットワークの接続制御を行う接続装置に対して特定のポート番号を通知し、このポート番号宛てに送信されてきたパケットを自装置に送信するよう設定するルーティング制御手段を備えることを特徴とする請求項 1 または 2 に記載の通信中継装置。

【請求項 10】

前記宅内ネットワーク及び前記宅外ネットワークの接続制御を行う接続装置に対して、自装置のグローバル IP アドレスを通知し、このグローバル IP アドレス宛てのパケットを自装置に送信するよう設定するルーティング制御手段を備えることを特徴とする請求項 1 または 2 に記載の通信中継装置。

【請求項 11】

前記ブリッジ処理手段は、さらに前記宅外ネットワークまたは前記宅内ネットワークの一方から入力されたデータの符号化変換、プロトコル変換、帯域変換の少なくとも 1 つの処理を行った後に、該データが入力されたのとは別のネットワークに対して前記変換後のデータを送信することを特徴とする、請求項 1 または 2 に記載の通信中継装置

【請求項 12】

宅内ネットワーク上の宅内通信装置と、
宅外ネットワーク上の宅外通信装置と、
前記宅内ネットワーク及び前記宅外ネットワークの間での情報送受信を中継する通信中継装置と、を備えた通信システムであって、
前記通信中継装置は、

前記宅内通信装置との間での著作権保護のための第1の認証鍵交換処理を行う第1の著作権保護手段と、

前記宅外通信装置との間での著作権保護のための前記第1の認証鍵交換処理とは異なる方式の第2の認証鍵交換処理を行う第2の著作権保護手段と、

前記宅外通信装置の識別情報を登録する識別情報記憶手段と、

前記宅外通信装置から接続要求があった場合には、

前記宅内ネットワークに接続要求を行った前記宅外通信装置が前記識別情報記憶手段に登録されていることを確認し、かつ前記接続要求についての前記第1及び第2の著作権保護手段による認証鍵交換が成功した場合に限り、前記宅内ネットワーク及び前記宅外ネットワークの間での情報の送受信を行うブリッジ処理手段と、を有することを特徴とする通信システム。

【請求項13】

宅外ネットワークに接続された宅外通信装置と、前記宅内ネットワークに接続された宅内通信装置との間で情報を中継する、宅内ネットワークに接続された通信中継装置において、

前記宅内ネットワーク上の宅内通信装置との間での著作権保護のための第1の認証鍵交換処理を行うステップと、

前記宅外ネットワーク上の宅外通信装置との間での著作権保護のための前記第1の認証鍵交換処理とは異なる方式の第2の認証鍵交換処理を行うステップと、

前記宅外通信装置の識別情報を登録するステップと、

前記宅外通信装置から接続要求があった場合には、

前記宅内ネットワークに接続要求を行った前記宅外通信装置の識別情報が登録されていることを確認し、かつ前記接続要求についての前記第1及び第2の認証鍵交換処理による認証鍵交換が成功した場合に限り、前記宅内ネットワーク及び前記宅外ネットワークの間での情報の送受信を行うステップと、を実行させるための通信制御プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、宅内ネットワークと宅外ネットワークとの間での情報送受信の仲介を行う通信中継装置、通信システム及び通信制御プログラムに関する。

【0002】

【従来の技術】

デジタル情報家電と呼ばれる商品が普及しつつある。これらは、デジタル放送の開始などに伴い、さらに普及が期待される商品群であり、デジタル放送対応テレビや、セットトップボックス、デジタルVTR、DVDプレーヤ、ハードディスクレコーダ等、デジタルデータやデジタルコンテンツを扱う商品すべてが対象となる。

【0003】

デジタルデータやデジタルコンテンツは、複製しても品質が劣化せず、複製も容易に行えるため、予め著作権保護に対する対策を考慮しておく必要がある。例えば、デジタルAV機器同士をつなぐデジタルネットワークであるIEEE1394には、認証・鍵交換機構や、データの暗号化の機能が兼ね備えられている。

【0004】

ここで、ある送信装置から、著作権保護が必要なAVデータを、受信装置に転送する場合を考える。ここで注意すべきは、個人(あるいは、拡大解釈して家族)の楽しむ範囲内でAVデータのやり取りを行うのが著作権保護の前提であり、第三者とのAVデータのやりとりは(著作権者の許可が伴わない限り)行われるべきでは無いという点である。

【0005】

ネットワーク上で著作権保護を実現するためのメカニズムとして、DTCPが知られている。DTCPとは、Digital Transmission Content Protectionの略で、IEEE1394やUSBなどでデファクトスタンダードとなっている著作権保護方式である。

【0006】

DTCPには、著作権保護が必要なAVデータなどのコンテンツに対して送信機器と受信機器との間で認証・鍵交換を行い、AVデータを暗号化して転送する仕組みが備わっている(例えば、非特許文献1を参照)。このDTCPを用いることにより、宅内のネットワーク(例えばIEEE1394ネットワーク)上で、著作権保護を保証し

た状態でのAVデータの伝送が可能になる。

【0007】

【非特許文献1】

<http://www.dtl.a.com>にて取得可能に開示されている文書

【0008】

【発明が解決しようとする課題】

一方、インターネットの普及により、デジタルデータを公衆網上でやり取りすることが一般的になってきた。このような状況下では、あるユーザが、別荘などのモバイル環境で、自宅にあるデータへのアクセスを要求する場合があります、このような要求を、著作権保護を理由に拒絶するのは、ユーザの利便性を損なう結果となる。

【0009】

しかしながら、現在のDTCPは、IEEE1394等のホームネットワークにその対象が限定されている。ユーザがモバイル環境で自宅にあるコンテンツにアクセスできるようにするには、例えば現在のDTCPを拡張して宅外でも使えるようにし、かつ宅内のDTCPで実現されている仕組みを宅外にも拡張する必要があるが、このような新たな仕組みについては従来何ら提案されていない。

【0010】

本発明は、このような点に鑑みてなされたものであり、その目的は、宅内ネットワーク間で送受信される情報を、著作権保護を図りつつ、宅外ネットワーク間でも送受信可能な通信中継装置、通信システム及び通信制御プログラムを提供することにある。

【0011】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、宅外ネットワークに接続された宅外通信装置と、宅内ネットワークに接続された宅内通信装置との間で情報を中継する、前記宅内ネットワークに接続された通信中継装置であって、

前記宅内ネットワーク上の宅内通信装置との間での著作権保護のための第1の認証鍵交換処理を行う第1の著作権保護手段と、

前記宅外ネットワーク上の宅外通信装置との間での著作権保護のための前記第1の認証鍵交換処理とは異なる方式の第2の認証鍵交換処理を行う第2の著作権保護手段と、

前記宅外通信装置の識別情報を登録する識別情報記憶手段と、

前記宅外通信装置から接続要求があった場合には、

前記宅内ネットワークに接続要求を行った前記宅外通信装置が前記識別情報記憶手段に登録されていることを確認し、かつ前記接続要求についての前記第1及び第2の著作権保護手段による認証鍵交換が成功した場合に限り、前記宅内ネットワーク及び前記宅外ネットワークの間での情報の送受信を行うブリッジ処理手段と、を備える。

【0012】

【発明の実施の形態】

以下、本発明に係る通信中継装置、通信システム及び通信制御プログラムについて、図面を参照しながら具体的に説明する。

【0013】

(第1の実施形態)

図1は本発明に係る通信システムの第1の実施形態の全体構成を示すブロック図である。図1の通信システムは、ユーザ宅1内に設置された送信装置2、ホームネットワーク3及び宅外DTCPブリッジ4と、ユーザ宅1にインターネット5を介して接続される宅外の受信装置6とを備えている。

【0014】

ホームネットワーク3の具体的な形態は特に問わず、例えば802.11無線LAN、イーサネットまたはIEEE1394などを採用可能である。ホームネットワーク3には、この他にも接続されている装置があってもよいが、ここでは記載を省略している。また、ホームネットワーク3上でインターネットプロトコルを使用する場合、特に具体的なプロトコルの種類は問わず、IPv4でもよいし、IPv6でもよい。

【0015】

宅外DTCPブリッジ4は、本実施形態の特徴的なものであり、ユーザ宅1内の送信装置2と宅外の受信装置6との間で、著作権保護が必要なAVデータの送受信を

仲介する。宅外DTCPブリッジ4には、ホームネットワーク3とインターネット5が接続されている。

【0016】

図2は宅外DTCPブリッジ4の内部構成を示すブロック図である。図2の宅外DTCPブリッジ4は、宅内ネットワークI/F部11と、DTCP関連パケットフィルタ12、13と、DTCP処理部14と、ホームルータ及びファイアウォール部15と、宅外ネットワークI/F部16とを有する。この他、宅外DTCPブリッジ4はモデム(ADSLモデムやFTTHの光・電気変換装置)を内蔵していてもよい。

【0017】

宅内ネットワークI/F部11は、無線LANやイーサネット、IEEE1394等のホームネットワーク3とのインタフェースを取るモジュールである。宅内ネットワークI/F部11とDTCP処理部14の間に位置するDTCP関連パケットフィルタ12は、宅内ネットワークI/F部11から入力されてきたパケットのうち、著作権保護処理であるDTCPの制御パケット(例えば、DTCPの認証鍵交換のためのパケット)や、著作権保護が必要なAVデータを含んだパケットを選択して、DTCP処理部14に振り分ける機能を持つ。また、DTCP関連パケットフィルタ12は、DTCP処理部14からのパケットと他のDTCP関連パケットフィルタ13から出力されてきたDTCPとは関連のないパケットとの多重化を行って、宅内ネットワークI/F部11に出力する。

【0018】

宅外ネットワークI/F部16は、インターネット5(公衆網)とのインタフェースを取るモジュールである。ホームルータ及びファイアウォール処理部15は、ホームルータ、NAT(ネットワークアドレス変換)、ファイアウォール等の機能を持つモジュールである。ホームルータ及びファイアウォール処理部15とDTCP処理部14の間に位置するDTCP関連パケットフィルタ13は、DTCP関連パケットフィルタ12と略同様の動作を行う。

【0019】

DTCP処理部14は、DTCPブリッジ処理部21と、自動構成認識及び家電制御用Webサーバ処理部22と、宅内側DTCP AKE処理部23と、宅外側DTCP AKE処理部

24と、宅外デバイス登録テーブル25と、ユーザ認証登録テーブル26とを有する。

【0020】

DTCP処理部14は、DTCP著作権保護に関する処理を行うが、その処理は主に、
(1) 宅内ネットワークI/F部11と宅外ネットワークI/F部16を介した送信装置2と受信装置6（あるいは他のDTCPブリッジ）との間でのDTCP認証鍵交換処理と、(2)著作権保護が必要なAVデータについての暗号化／復号化等の処理と、(3) DTCPブリッジ処理と、(4)必要に応じて行われるAVデータの符号化変換処理やプロトコル変換処理、帯域変換処理などである。

【0021】

宅内側DTCP AKE処理部23は、宅内側のDTCP認証・鍵交換処理を行う。ここで、AKEとは、Authentication and key exchangeの略である。DTCP認証鍵交換は、例えばIPパケット上の特定のポート番号（DTCP-AKEに割り当てられたポート番号）で示されるパケット、あるいは無線LANやイーサネット上のDTCP専用のフレーム、あるいはIEEE1394のAV/Cパケットのセキュリティコマンド等を使って行われる。宅内にて行われる認証・鍵交換は、これが成立する範囲を家庭内に限定するために、例えばTTL（Time To Live）の値を1にする、IPアドレスとしてリンクローカルアドレスを使う（特開2001-285284号公報参照）、伝送パケットにIPパケットの代わりにイーサネットフレームを使う、または、パケットが届くまでのタイムアウト時間を制限する（特願2002-19135号参照）等の工夫が施されていてもよい。

【0022】

宅外側DTCP AKE処理部24は、宅外側のDTCP認証・鍵交換処理を行う。宅外のDTCP認証鍵交換は、例えばIPパケット上の特定のポート番号で示されるパケット、あるいは、HTMLの特定のラベル（例えばX-DTCP）を使ってDTCPパケットであることを示した上でHTTPを使ってやり取りされる。HTTPを使って送受すると、認証鍵交換の経路途中にプロキシサーバやネットワークアドレス変換装置（NAT）が存在していても、通信を継続できる場合がある、という利点がある。宅外のDTCP認証鍵交換は、通信相手となる装置（本実施形態の場合は受信装置6）が、DTCP

ブリッジからどれだけ離れた場所に位置しているかわからないため、例えばTTLの値等に制限を設ける必要はないし、グローバルIPアドレスで通信が成立していてもよい。

【 0 0 2 3 】

DTCPには、シンクリミテーションなる仕組みが定義されている。即ち、同時に通信できる装置の数（あるいは、同一AVストリームを同時にやり取りできる装置の数）を、一定以下の数に制限する仕組みである。シンクリミテーションの仕組みを導入しない場合、事実上無制限の数の装置が同一ネットワーク上に接続されて、1本のAVストリームから、大量の接続装置へのAVデータのコピーが行われ、コピーコンテンツが大量に生成されてしまうため、このような不具合を未然に防止するためにシンクリミテーションが導入される。

【 0 0 2 4 】

本実施形態の宅外DTCPブリッジ4は、シンクリミテーションの仕組みを更に強化し、以下の(1)～(4)の特徴を持つ。なお、(1)～(4)の一部だけを実現してもよい。

【 0 0 2 5 】

(1) 宅外側からアクセスされるデバイス（例えば、受信装置6）を予め宅外デバイス登録テーブル25に登録しておき、この登録テーブルに登録されたデバイス以外からの通信（認証鍵交換の申し込み）を拒否する。

【 0 0 2 6 】

(2) 宅外デバイス登録テーブル25に登録できるデバイス数を一定以下（例えば16台）に制限する（つまり、テーブルの大きさに上限がある）。

【 0 0 2 7 】

(3) 一度登録したデバイスは、永久的に宅外デバイス登録テーブル25に登録される（たとえ電源がオフにされたり、電力供給がカットされたとしても登録は消えない）。

【 0 0 2 8 】

(4) 宅外デバイス登録テーブルへの登録は、宅内からのみ行えるようにする。

【 0 0 2 9 】

図 3 は宅外デバイス登録テーブル 2 5 のデータ構成の一例を示す図である。図示のように、宅外デバイス登録テーブル 2 5 は、必須項目とオプション項目に分けられ、必須項目には、各デバイス（ここでは、受信装置 6）に必ず割り当てられる著作権保護のための Certificate（機器証明書）に記述されているデバイス ID と、その装置の固有 ID である MAC アドレス（例えば IEEE802 アドレス等のように、一般的には、アドレス種別と ID の組合せで表現される）との少なくとも一方が登録される。オプション項目には、各受信装置 6 の接続開始日時、宅外デバイス登録テーブル 2 5 への登録日時、及び接続状態が登録される。なお、必須項目は必ず必要であるが、オプション項目は必要に応じて設ければよい。

【 0 0 3 0 】

宅外デバイス登録テーブル 2 5 に予め登録された DTCP デバイスのみが、宅外 DTCP ブリッジ 4 を介したユーザ宅 1 との DTCP ブリッジ通信に参加することができる。つまり、予め登録されたデバイス以外は DTCP ブリッジ通信を行えない。

【 0 0 3 1 】

また、上記 (2) の特徴により、通信可能なデバイスは所定数に制限されるため、通信のたびに宅外デバイス登録テーブル 2 5 の内容を書き換え、その都度異なるデバイスに対して通信を許可し、その結果、実質的に無数のデバイスに対して（時間をずらして）データを送信するようなことは不可能になる。したがって、ユーザによる不正コピーを防止でき、かつ不特定多数の装置が宅外 DTCP ブリッジ 4 に接続されるおそれもなくなる。つまり、本実施形態によれば、宅外接続が可能な受信装置 6 の数を上述した (2) の数に確実に制限できる。

【 0 0 3 2 】

宅外デバイス登録テーブル 2 5 は、ユーザが改変できないような構成にするのが望ましい。これは、ユーザによる改変ができると、その都度、通信したいデバイスを登録することにより、実質的に無制限の数のデバイスとの通信が可能になってしまうためである。

【 0 0 3 3 】

ユーザ認証登録テーブル 2 6 には、宅外 DTCP ブリッジ 4 に接続可能な各受信装置 6 のユーザ ID とパスワードが登録される。宅外側 DTCP AKE 処理部 2 4 は、宅外

側からDTCP認証鍵交換の要求があったときに、要求を行った受信装置6のユーザIDとパスワードがユーザ認証登録テーブル26に登録されているか否かを確認するユーザ認証を行い、ユーザ認証に成功した場合のみDTCP認証・鍵交換処理を行う。

【0034】

これにより、DTCPには準拠しているものの、ユーザIDやパスワードが登録されていない他人のDTCPデバイスからの接続要求を拒否することができる。

【0035】

宅外デバイス登録テーブル25とユーザ認証登録テーブル26はいずれも、宅外からのアクセスでテーブルを改変できないようになっており、宅外デバイス登録テーブル25は宅内からのユーザアクセスによっても改変できないようになっている。

【0036】

DTCPブリッジ処理部21は、宅内側のネットワークと宅外側のネットワークを論理的に接続し、例えば「送信装置2からの暗号化AVデータの受信とその復号化（宅内側DTCP AKE処理部23が得た鍵を用いた復号）、再暗号化（宅外側DTCP AKE処理部24により合意した鍵を用いた暗号化）、及び受信装置6に対する暗号化AVデータの送信等のブリッジ処理を行う。

【0037】

自動構成認識及び家電制御用Webサーバ処理部22は、宅内ネットワーク内に存在する、宅外のデバイスまたは宅外DTCPブリッジ4処理部から制御・監視が可能なデバイスを自動的に構成認識し、このデバイスの制御・監視及び管理用のWebページを自動的に作成する機能と、作成したWebページを内部のWebサーバにより宅外側に公開する機能とを持つ。もちろん、作成したWebページを宅内側に公開してもよい。

【0038】

図4はユーザ宅1内の送信装置2の内部構成の一例を示すブロック図である。図示のように、送信装置2は、ネットワークインターフェース部31と、通信処理を実行する通信処理部32と、本送信装置2のDTCPデバイスIDを記録するDTCP

デバイスID記録部 3 3 と、宅外DTCPブリッジ 4 から送信されたDTCPデバイスID及びMACアドレスを処理するID処理部 3 4 と、DTCPデバイスID及びMACアドレスをIDリストとして登録したり、宅内DTCPブリッジ等から受信したIDとIDリストに登録された値との比較処理を行なうID管理部 3 5 と、著作権保護を図るためにDTCP認証・鍵交換処理を行う認証・鍵交換処理部 3 6 と、送信するデータを暗号・復号化する暗号処理部 3 7 と、宅外DTCPブリッジ 4 に送信するAVコンテンツデータやDTCP管理データを通信パケットに変換するパケット処理部 3 8 と、コンテンツを蓄積するコンテンツ供給部 3 9 とを有する。

【 0 0 3 9 】

ここで、DTCPデバイスIDとは、DTCPデバイスの識別番号である。全世界のDTCPデバイスがそれぞれ唯一の値となるように、予めDTCPデバイスに割り当てられた値であるのが望ましい。

【 0 0 4 0 】

図 5 は宅外の受信装置 6 の内部構成の一例を示すブロック図である。図示のように、受信装置 6 は、ネットワーク処理を実行するネットワークインターフェース部 4 1 と、通信処理を実行する通信処理部 4 2 と、受信装置 6 のDTCPデバイスIDを記録するデバイスID記録部 4 3 と、デバイス固有の値（MACアドレス）を取得するデバイス固有ID取得部 4 4 と、取得したデバイスIDを送信するデバイスID送信部 4 5 と、著作権保護を図るためにDTCP認証・鍵交換処理を行う認証・鍵交換処理部 4 6 と、送信するデータを暗号・復号化する暗号処理部 4 7 と、受信したパケットをAVコンテンツデータやDTCP管理データに変換するパケット処理部 4 8 と、パケットを表示装置などに出力したり蓄積する処理を行なうコンテンツ処理部 4 9 と、本受信装置 6 を宅内で使用するのか宅外で使用するのかを指定する宅内・宅外接続指定部 5 0 と、を有する。

【 0 0 4 1 】

宅内・宅外接続指定部 5 0 は、受信装置 6 をユーザの宅内にて使用する場合（宅外DTCPブリッジ 4 を介さなくても送信装置 2 と通信が可能な状態）と、受信装置 6 をユーザ宅外にて使用する場合（宅外DTCPブリッジ 4 を介さないと送信装置 2 との通信ができない状態）とを指定する機能を有する。

【0042】

受信装置 6 を宅内で使用する場合、暗号処理部 47 と認証・鍵交換処理部 46 は、（例えば、TTL=1のみ許可する等の）宅内向けのDTCPプロトコルを用いて通信を行う。また、受信装置 6 を宅外で使用する場合、暗号処理部 47 と認証・鍵交換処理部 46 は、（例えば、予めユーザ認証を行うとか、TTL=複数を許可する等の）宅外向けのDTCPプロトコルを用いて通信を行う。

【0043】

宅内・宅外接続指定部 50 による宅内／宅外の切換指定は、ユーザが手動で行ってもよいし、GPSなどを用いて、受信装置 6 の場所や設置状況を受信装置 6 自身で自動的に判断した上で切り替えを行ってもよい。

【0044】

デバイス固有ID取得部 44 が取得するデバイス固有の値とは、例えばネットワークデバイス製造ベンダが管理し、デバイスごとに一意となる値を割り振って物理的にそのデバイスに記録されたネットワークインターフェースのMACアドレスなどを指す。例えばイーサネットMACアドレスやIEEE1394で定められているnode_vender_idやchip_idまたはそれらを組み合わせた値などである。

【0045】

上述したように、ユーザ宅 1 内の送信装置 2 から、ホームネットワーク 3（家庭網）、宅外DTCPブリッジ 4 及びインターネット 5（公衆網）を介して、ユーザ宅外の受信装置 6 にAVコンテンツを送信する場合の処理手順をより詳しく説明する。

【0046】

本実施形態では、まず、受信装置 6 を宅外DTCPブリッジ 4 に登録する。より詳細には、宅外DTCPブリッジ 4 内の宅外デバイス登録テーブル 25 に受信装置 6 を登録する。宅外デバイス登録テーブル 25 への登録手順として、図 6 に示す 3 通りが考えられる。

【0047】

第 1 の登録手順は、予め宅外DTCPブリッジ 4 の宅外デバイス登録テーブル 25 に、手入力で、受信装置 6 を登録する方法である。より具体的には、例えば宅外

DTCPブリッジ4に備え付けてある何らかのユーザインタフェース（液晶画面とボタン等）を通して登録してもよいし、ホームネットワーク3を経由して、PCなりテレビ（とりモコン）なりのユーザインタフェースを使用して入力してもよい。

【0048】

第1の登録手順の場合、ユーザは、まず、宅外からの接続を行いたいデバイス（本実施形態の場合、受信装置6）のデバイスIDと固有ID（本実施形態の場合MACアドレスの値）を、何らかの方法で入手する（ステップS1）。

【0049】

次に、必要に応じて、宅外DTCPブリッジ4を宅外デバイス登録テーブル25に登録可能なモードに設定する（ステップS2）。次に、ステップS1で入手したデバイスIDと固有ID（MACアドレス）を宅外デバイス登録テーブル25に登録する（ステップS3）。登録の際は、キーボード等を用いて手入力してもよいし、デバイスID等を自動設定してもよい。

【0050】

宅外デバイス登録テーブル25にいったん登録すると、その登録内容は永続的に記憶され（ステップS4）、ユーザが事後的に変更できないようにするのが望ましい。その理由は、消去や再登録の繰り返しにより、複数回登録できてしまうと、登録の繰り返しにより、實際上無限回数の宅外デバイスに対する情報送信が可能になってしまうためである。

【0051】

また、これと同時に、ユーザ認証登録テーブル26に、ユーザIDとパスワード等の、ユーザ認証に関わる部分の登録を行ってもよい（ステップS5）。

【0052】

第2の登録手順は、ホームネットワーク3に受信装置6を接続し（ステップS11）、宅外DTCPブリッジ4を登録モードに変更した上で（ステップS12）、宅外DTCPブリッジ4と受信装置6間でDTCP認証鍵交換を実行させて（ステップS13）、その結果（受信装置6のDTCPデバイスIDと固有ID）を宅外DTCPブリッジ4が、宅外デバイス登録テーブル25に記憶するものである（ステップS14）。なお、受信装置がDTCPデバイスIDを2つ以上持っている場合には、宅外通信用

に用いるDTCPデバイスIDを、宅外デバイス登録テーブル25に記憶するようにする。

【0053】

なお、固有ID（MACアドレス）の値の同一性を確保するため、この場合は、ホームネットワーク3のインタフェースと宅外のインターネット5（公衆網）とのインタフェースが同一のもの（例えば無線LANインタフェース等）であるのが望ましい。

【0054】

この場合も、宅外デバイス登録テーブル25にいったん登録すると、ユーザが事後的に変更できないようにするのが望ましい。また、必要に応じて、ユーザIDやパスワード等のユーザ認証情報をユーザ認証登録テーブル26に登録してもよい。

【0055】

第3の登録手順は、予め宅内側から、宅外DTCPブリッジ4の宅外デバイス登録テーブル25に登録を行うのではなく、宅外からのアドホックな登録を行う方法である。

【0056】

宅外DTCPブリッジ4は、例えば常に宅外からの新規のデバイスの接続を受け付け可能な状態になっており、登録の要求やDTCP認証鍵交換の要求が来ると、そのデバイスのデバイスIDと固有ID（本実施形態の場合はMACアドレス）の値を新規に宅外デバイス登録テーブル25に登録する（ステップS21）。この登録は、前述のように永続的に行われ、その登録可能数には上限があるため、無制限な任意の数の宅外デバイスを登録することはできない。

【0057】

その後、宅外DTCPブリッジ4は、宅外の受信装置6の接続要求を受け付ける（ステップS22）。宅外の受信装置6が宅外DTCPブリッジ4に対して接続要求を行うと、この受信装置6にユーザ認証を求め（ステップS23）、これに正確に応じられた受信装置6のみを、宅外デバイス登録テーブル25に登録する（ステップS24）。

【0058】

図7は、図6の第1～第3の処理手順のいずれかで宅外デバイス登録テーブル25に登録された受信装置6を実際に宅外で使用して、ユーザ宅1との通信を行う場合の処理手順の一例を示すシーケンス図である。

【0059】

まず、宅外DTCPブリッジ4は、ホームネットワーク3に接続された（あるいは電源が投入された）送信装置2を、自動構成認識手順を用いて認識する（ステップS31）。次に、宅外DTCPブリッジ4は、送信装置2を制御可能なWebページを作成する（ステップS32）。このWebページには、再生ボタンやコンテンツ選択ボタンなどが含まれる。

【0060】

次に、宅外DTCPブリッジ4は、作成したWebページを宅外側に公開する（ステップS33）。なお、このWebページには、上述したユーザ認証など、何らかのユーザ認証を通った宅外デバイス（受信装置2など）のみがアクセスできるようにするのが望ましい。

【0061】

さて、宅外に設置された受信装置6が、ユーザ宅1内の送信装置2内のAVコンテンツのダウンロードを希望しているとする（ステップS34）。ユーザは、受信装置6をインターネット5に接続し、受信装置6内に予め記憶してあるユーザ宅1の宅外DTCPブリッジ4にアクセスを行う。もちろん、ユーザの手入力によって、宅外DTCPブリッジ4のドメインネームなり、IPアドレスなりを指定してもよい。この場合、宅外DTCPブリッジ4に、DDNS（動的ドメインネームサービス）を適用してもよい。

【0062】

受信装置6が宅外DTCPブリッジ4にアクセスする手順は以下の通りである。まず、受信装置6と宅外DTCPとの間でユーザ認証を行う（ステップS35）。ユーザ認証が通ると、宅外DTCPブリッジ4は、自動構成認識及び家電制御Webサーバ処理部22を介して、送信装置2の制御画面を受信装置6に送信する（ステップS36）。この制御画面を受信した受信装置6は、送信装置2が提供可能な適当

なAVコンテンツをWeb画面上で選択し、選択した特定コンテンツの送信要求を宅外DTCPブリッジ4に送信する（ステップS37）。

【0063】

宅外DTCPブリッジ4は、必要に応じて送信装置2との間で通信を行い、ユーザ（受信装置6）が選択したAVコンテンツの送信には、著作権保護がかかっており、予めDTCP認証鍵交換が必要であることを認識すると、DTCP認証鍵交換（宅外仕様）が必要であることを受信装置6に対して通知する（ステップS38）。

【0064】

この通知を受けて、宅外DTCPブリッジ4と受信装置6間で、宅外DTCPの認証鍵交換処理が行われる（ステップS39）。この際、受信装置6の機器証明書（Certificate）には、受信装置6のデバイスIDと固有ID（MACアドレス等）が登録されている。よい。

【0065】

宅外DTCPブリッジ4は、受信装置6（のデバイスIDと固有ID=MACアドレス）が宅外デバイス登録テーブル25に登録されているか否かを確認し（ステップS40）、その確認ができた場合には、「送信装置2と宅外DTCPブリッジ4間の認証鍵交換、及びAVコンテンツの暗号化・伝送・復号化処理」と、「宅外DTCPブリッジ4と受信装置6間の認証鍵交換、及びAVコンテンツの暗号化・伝送・復号化処理」とを結び付ける（ステップS41～S43）。即ち、送信装置2と宅外DTCPブリッジ4間で転送される暗号化コンテンツを、送信装置2と宅外DTCPブリッジ4間で認証鍵交換される鍵を用いて復号化し（ステップS41）、復号化したコンテンツを宅外DTCPブリッジ4と受信装置6間で認証鍵交換される鍵を用いて再暗号化し（ステップS42）、再暗号化したコンテンツを受信装置6に対して送信するように、DTCPブリッジ処理部21の設定を行う（ステップS43）。

【0066】

受信装置6から、著作権保護が必要なコンテンツの送信要求があると（ステップS44）、宅外DTCPブリッジ4は送信装置2にそのコンテンツの送信要求を伝達する（ステップS45）。

【0067】

送信装置 2 から送信されてきた、暗号化されたAVデータは（ステップ S 4 6）、内部でトランスクリプト処理（暗号の復号化と、再暗号化）がなされた上で（ステップ S 4 7）、受信装置 6 に対して送信される（ステップ S 4 8）。

【 0 0 6 8 】

その際に、ホームネットワーク 3 の帯域と、インターネット 5（公衆網）の帯域（特に、加入者線の帯域）の間にギャップがある場合には、宅内DTCPブリッジのDTCPブリッジ処理部 2 1 内にて、復号化されたAVデータのトランスコード、つまり符号化方式や圧縮帯域等の変換を行ってもよい。例えば、ホームネットワーク 3 が100Mbpsの伝送能力を持つイーサネットで、公衆網（インターネット 5）の加入者線が6 Mbpsの伝送能力を持つADSLである場合などには、ホームネットワーク 3 では25Mbps超のMPEG2映像の形で（暗号化された上で）送信され、これを宅内DTCPブリッジ内にて（復号化した上で）1 Mbps程度のMPEG4等の異なる符号化方式、あるいは2 Mbps程度のMPEG2等の圧縮帯域の変更などを行った上で、これを（再暗号化した上で）インターネット 5 に対して伝送してもよい。

【 0 0 6 9 】

また、送信装置 2 と宅外DTCPブリッジ 4 間のAVデータ伝送用プロトコルはRTP（リアルタイムトランスポートプロトコル）、宅外DTCPブリッジ 4 と受信装置 6 間はHTTP（ハイパーテキストトランスファープロトコル）といったように、AVデータ伝送用プロトコルの変換を、DTCP処理部 1 4 内にて行ってもよい。

【 0 0 7 0 】

このように、第 1 の実施形態では、ユーザ宅 1 内の宅外DTCPブリッジ 4 に宅外デバイス登録テーブル 2 5 を設け、このテーブルに予め登録された受信装置 6 のみにユーザ宅 1 内からのコンテンツ送信を許可するため、著作権保護を図る必要のあるコンテンツの不正コピーや不正取得を防止しつつ、正規のユーザに対して宅外でもコンテンツを利用できる機会を与えることができ、ユーザの利便性が向上する。

【 0 0 7 1 】

また、宅外DTCPブリッジ 4 にユーザ認証登録テーブル 2 6 を設けることにより、ユーザ認証を通った宅外の受信装置 6 のみにコンテンツを送信でき、著作権保

護をより強化することができる。

【0072】

さらに、ユーザ宅1内と宅外でAVデータ伝送用のプロトコルや、接続されているネットワークの属性が異なっている場合、この違いを宅外DTCPブリッジ4で吸収できるため、送信装置2や受信装置6の種類にあまり限定されずにコンテンツを送受信できる。

【0073】

(第2の実施形態)

第1の実施形態では、宅外DTCPブリッジ4にホームルータが内蔵されている例を説明したが、宅外DTCPブリッジ4とは別個にホームルータを設けてもよい。

【0074】

図8は本発明に係る通信システムの第2の実施形態の全体構成を示すブロック図、図9は宅外DTCPブリッジ4の内部構成の一例を示すブロック図である。図8及び図9では図1及び図2と共通する構成部分には同一符号を付しており、以下では相違点を中心に説明する。

【0075】

図8に示すように、ユーザ宅1内の宅外DTCPブリッジ4aとは別個にホームルータ7が設けられており、宅外DTCPブリッジ4aの内部には、ホームルータ7に対する各種設定を行うホームルータ及びファイアウォール設定部17が設けられている。これ以外の構成は第1の実施形態と同様である。

【0076】

宅外の受信装置6から宅外DTCPブリッジ4に対してアクセスを行う方法として、以下の3通りがある。(1)ホームルータ内にNAT(ネットワークアドレス変換)があり、受信装置6はホームルータの特定ポートにアクセスすることによって宅外DTCPブリッジ4にアクセスすることができる。(2)宅外DTCPブリッジ4もグローバルユニークなIPアドレスを持っており、ホームルータに特定ポートに対する「穴」が開いているために、受信装置6から宅外DTCPブリッジ4に直接アクセスすることができる。(3)(1)と(2)を組み合わせた方法である。

【0077】

(3)の場合、図10に示すように、UPnP(ユニバーサルプラグアンドプレイ、例えば<http://www.upnp.org>を参照)を用いて、宅外DTCPブリッジ4がホームルータに対してHTTP用ポートの開放要求を行う(ステップS61)。この要求を受けて、ホームルータ7は、宅外DTCPブリッジ4向けのHTTPポートをインターネット5からアクセスできるように設定する(ステップS62)。その後、ホームルータ7は、HTTP用ポートの開放完了を宅外DTCPブリッジ4に送信する(ステップS63)。

【0078】

次に、宅外DTCPブリッジ4は、ホームルータ7にDTCP用ポートの開放要求を行う(ステップS64)。この要求を受けて、ホームルータ7は、宅外DTCPブリッジ4向けのDTCPポートをインターネット5からアクセスできるように設定する(ステップS65)。その後、ホームルータ7は、DTCP用ポートの開放完了を宅外DTCPブリッジ4に送信する(ステップS66)。

【0079】

上述した(1)の場合、宅外DTCPブリッジ4からホームルータに対して、特定のポート番号(DTCP認証鍵交換と、AVデータ伝送、HTTPに使われるTCP、又はUDPのポート番号)を通知して、このポート番号宛てにきたパケットを宅外DTCPブリッジ4に送信するように設定を行う。

【0080】

また、(2)の場合、宅外DTCPブリッジ4からホームルータに対して、宅外DTCPブリッジ4自身がグローバルIPアドレスを有することを通知し、宅外DTCPブリッジ4宛でのパケットを正しくルーティングするように設定を行う。

【0081】

上記以外の処理、すなわち送信装置2と宅外DTCPブリッジ4、及び受信装置6間でのDTCP認証鍵交換、暗号化AVデータ転送、宅外DTCPブリッジ4内でのDTCPブリッジ等は第1の実施例と同様であるため、説明を省略する。

【0082】

このように、第2の実施形態では、DTCPブリッジとは別個にホームルータを設けるため、すでにホームルータ7を備えている通信システムでも、そのホームル

ータ 7 を利用して本実施形態の通信システムを構築でき、設備コストの上昇を抑制できる。

【0083】

上述した第 1 及び第 2 の実施形態では、ユーザ宅 1 内から宅外に情報を送信する例を説明したが、その逆に、宅外デバイスからユーザ宅 1 にコンテンツを送信してもよい。宅外からユーザ宅 1 にコンテンツを送信する場合も、宅外 DTCP ブリッジ 4 内の宅外デバイス登録テーブル 25 に予め登録されている宅外デバイスのみ、ユーザ宅 1 へのコンテンツの送信を許可でき、コンテンツの著作権保護が図れる。

【0084】

上述した各実施形態で説明した宅外 DTCP ブリッジ 4 は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、宅外 DTCP ブリッジ 4 の機能を実現するプログラムをフロッピーディスクや CD-ROM 等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【0085】

また、宅外 DTCP ブリッジ 4 の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

【0086】

【発明の効果】

以上詳細に説明したように、本発明によれば、宅外通信装置が第 1 の登録手段に登録されていない場合には、宅内ネットワーク及び宅外ネットワーク間での通信を認めないため、情報の不正コピーや不正取得を確実に防止できる。また、第 1 の登録手段に登録され、かつ第 1 及び第 2 の著作権保護手段による認証鍵交換に成功した場合には、宅内ネットワーク及び宅外ネットワーク間での通信を認めるため、正規ユーザが宅外で宅内の情報を利用でき、ユーザの利便性が向上する

。 【図面の簡単な説明】

【図 1】

本発明に係る通信システムの第 1 の実施形態の全体構成を示すブロック図。

【図 2】

宅外DTCPブリッジの内部構成を示すブロック図。

【図 3】

宅外デバイス登録テーブルのデータ構成の一例を示す図。

【図 4】

ユーザ宅 1 内の送信装置の内部構成の一例を示すブロック図。

【図 5】

宅外の受信装置の内部構成の一例を示すブロック図。

【図 6】

宅外デバイス登録テーブルへの登録手順を示すフローチャート。

【図 7】

図 6 の第 1 ～第 3 の処理手順のいずれかで宅外デバイス登録テーブルに登録された受信装置 6 を実際に宅外で使用して、ユーザ宅 1 との通信を行う場合の処理手順の一例を示すシーケンス図。

【図 8】

本発明に係る通信システムの第 2 の実施形態の全体構成を示すブロック図。

【図 9】

宅外DTCPブリッジの内部構成の一例を示すブロック図。

【図 10】

第 2 の実施形態における宅内DTCPブリッジとホームルータ間のシーケンス図。

【符号の説明】

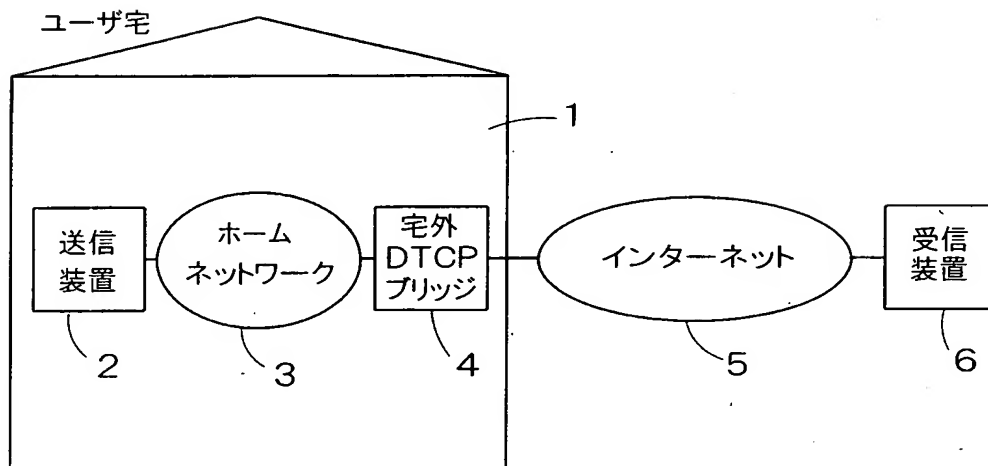
- 1 ユーザ宅
- 2 送信装置
- 3 ホームネットワーク
- 4 宅外DTCPブリッジ

- 5 インターネット
- 6 受信装置
 - 1 1 宅内ネットワークI/F
 - 1 2, 1 3 DTCP関連パケットフィルタ
 - 1 4 DTCP処理部
 - 1 5 ホームルータ及びファイアウォール処理部
 - 1 6 宅外ネットワークI/F部
 - 2 1 DTCPブリッジ処理部
 - 2 2 自動構成認識及び家電制御用Webサーバ処理部
 - 2 3 宅内側DTCP AKE処理部
 - 2 4 宅外側DTCP AKE処理部
 - 2 5 宅外デバイス登録テーブル
 - 2 6 ユーザ認証登録テーブル
 - 3 1 ネットワークインタフェース部
 - 3 2 通信処理部
 - 3 3 DTCPデバイスID記録部
 - 3 4 ID処理部
 - 3 5 ID管理部
 - 3 6 認証・鍵交換処理部
 - 3 7 暗号処理部
 - 3 8 パケット処理部
 - 3 9 コンテンツ供給部
 - 4 1 ネットワークインタフェース部
 - 4 2 通信処理部
 - 4 3 DTCPデバイスID記録部
 - 4 4 デバイス固有ID取得部
 - 4 5 デバイスID送信部
 - 4 6 認証・鍵交換処理部
 - 4 7 暗号処理部

- 4 8 パケット処理部
- 4 9 コンテンツ処理部
- 5 0 宅内・宅外接続指定部

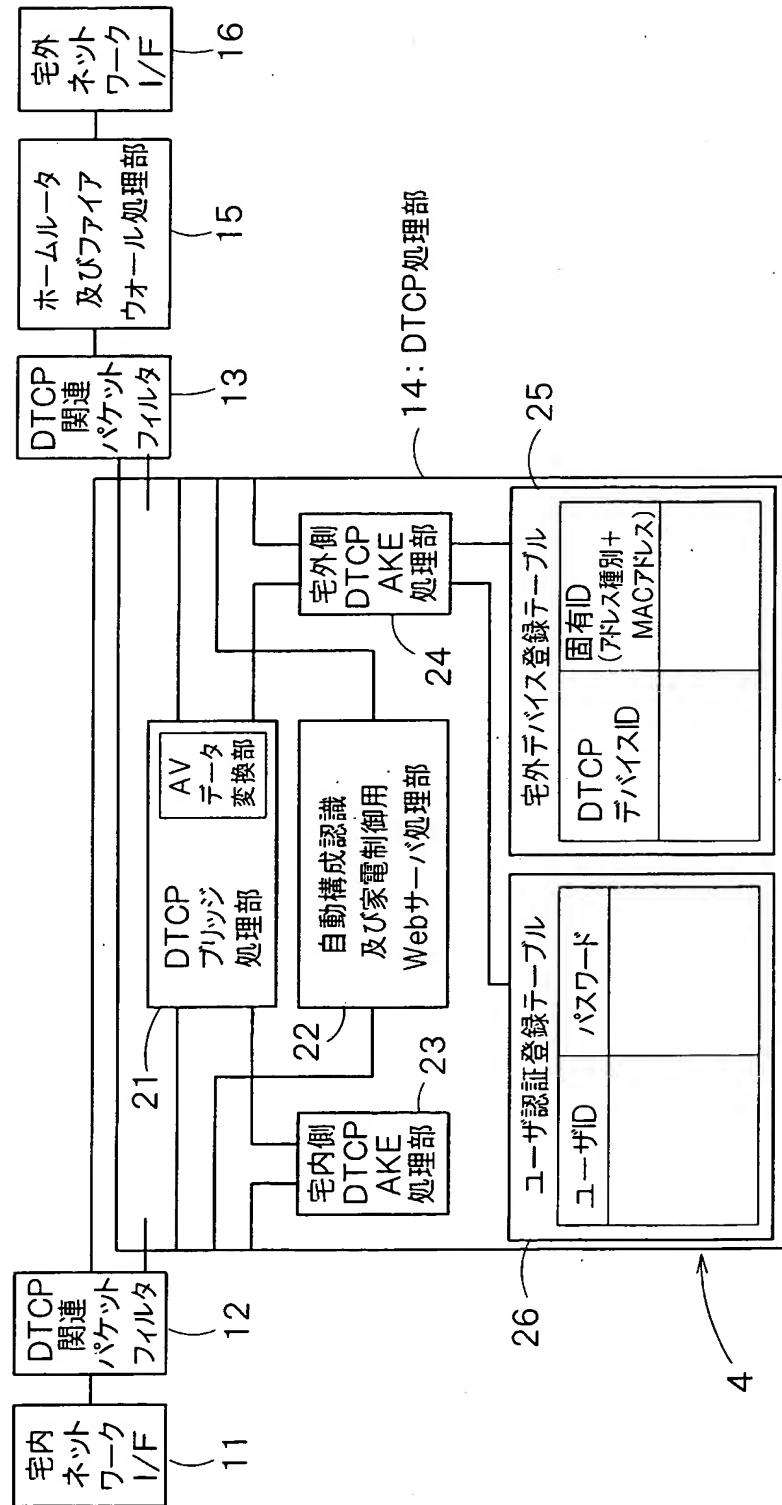
【書類名】 図面

【図 1】

第1の実施形態の全体構成

【図 2】

宅外DTCPブリッジの内部構成

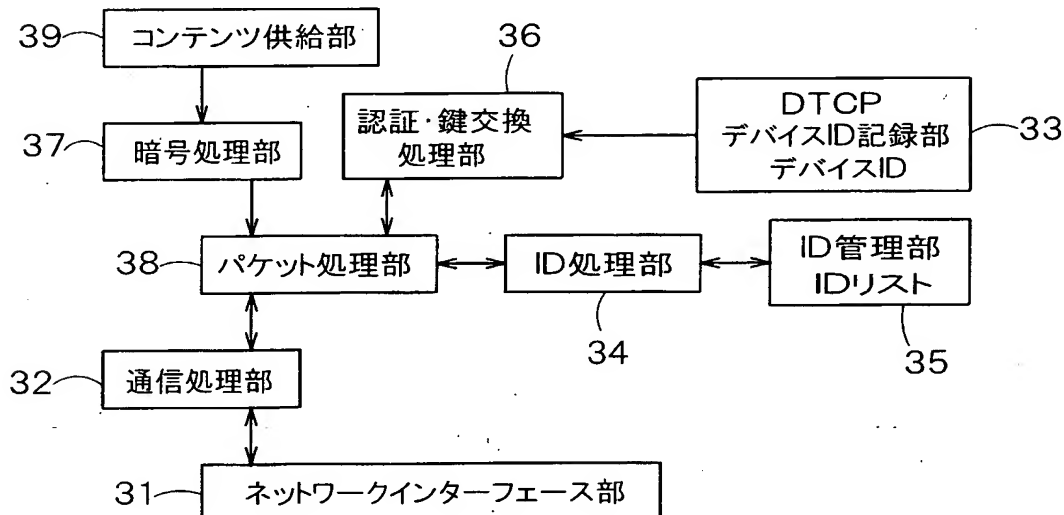


【図3】

宅外デバイス登録テーブル

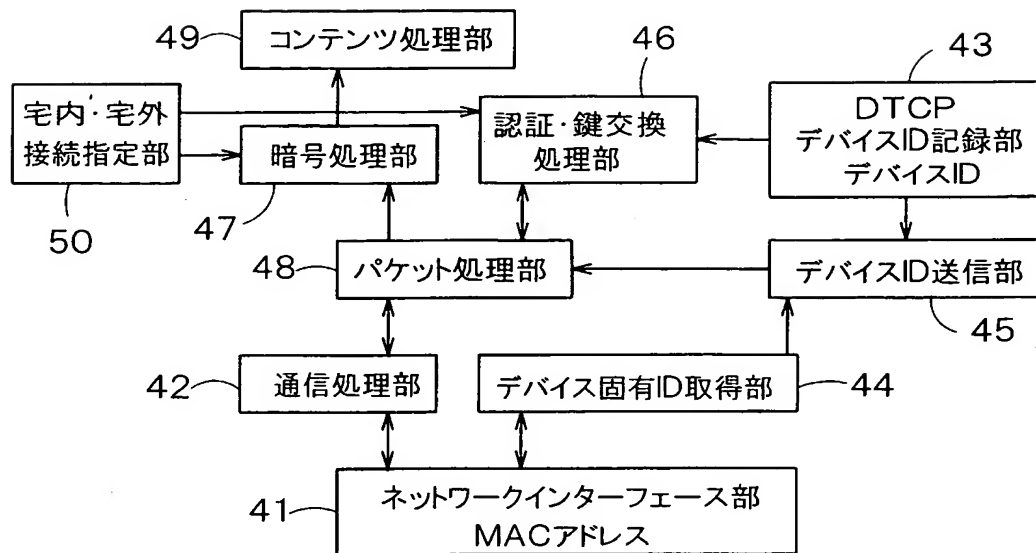
必須項目			オプション項目		
受信装置1	デバイスID	AA	接続開始日時	記録日時	接続状態
	固有ID	XX	×日○時△分	×日○時×分	接続中
受信装置2	デバイスID	AA	□日△時×分	□日△時○分	---
	固有ID	YY			
受信装置3	デバイスID	BB	×日○時□分	○日×時□分	接続中
	固有ID	ZZ			
...			...		

【図4】

送信装置の内部構成

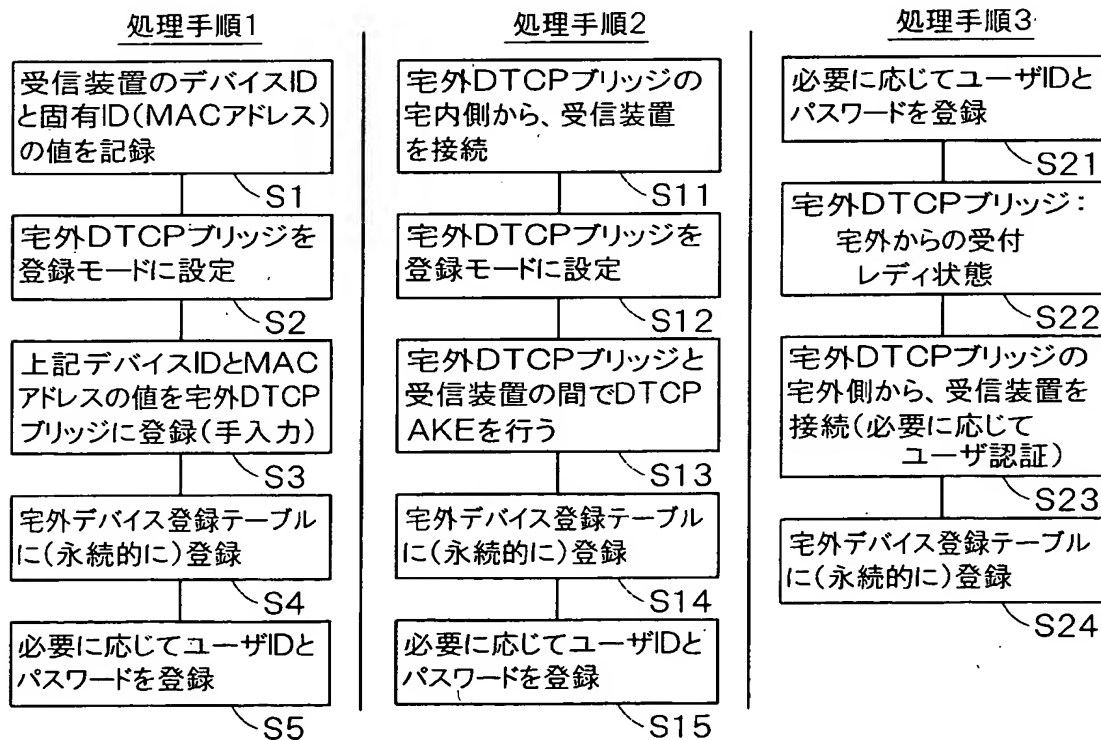
【図5】

受信装置の内部構成



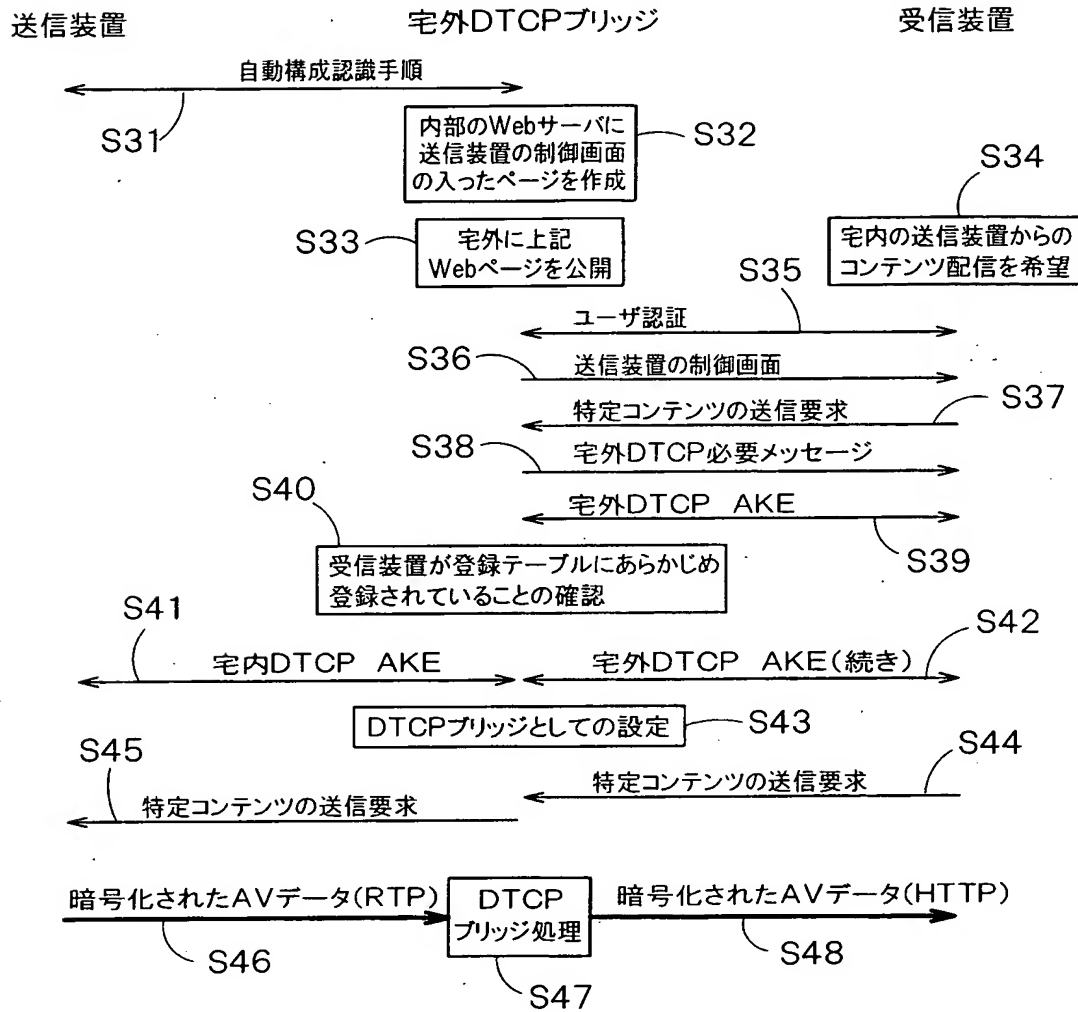
【図6】

宅外デバイス登録テーブルへの登録方法



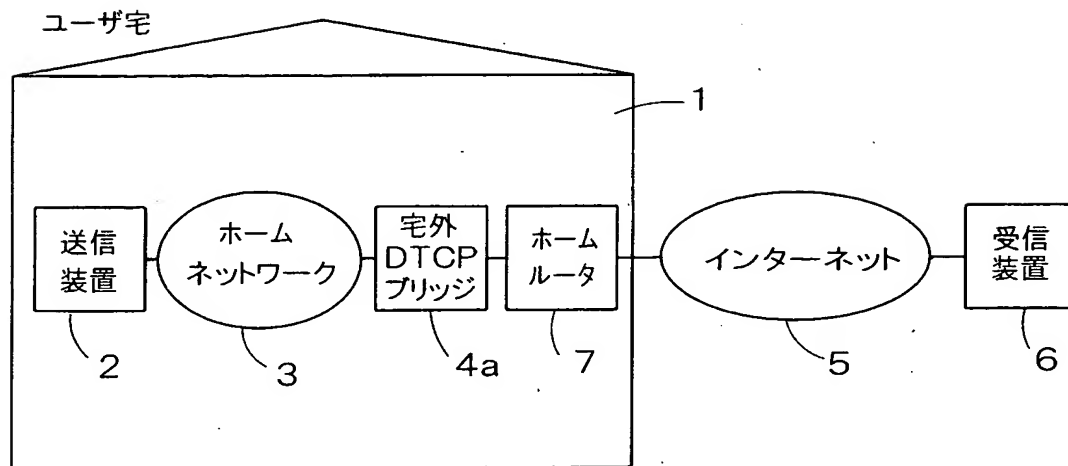
【図 7】

第1の実施形態の処理シーケンス



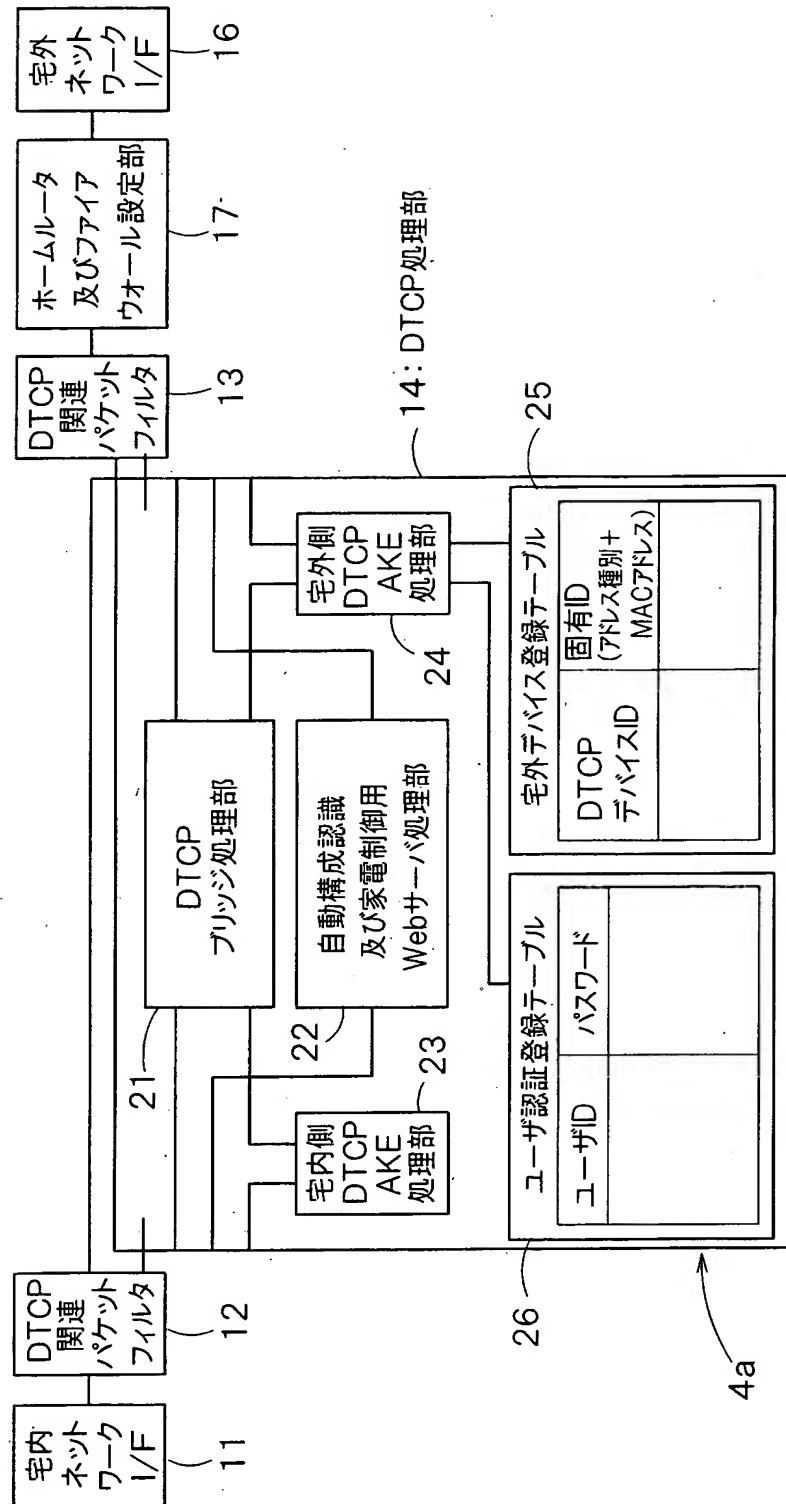
【図 8】

第2の実施形態の全体構成

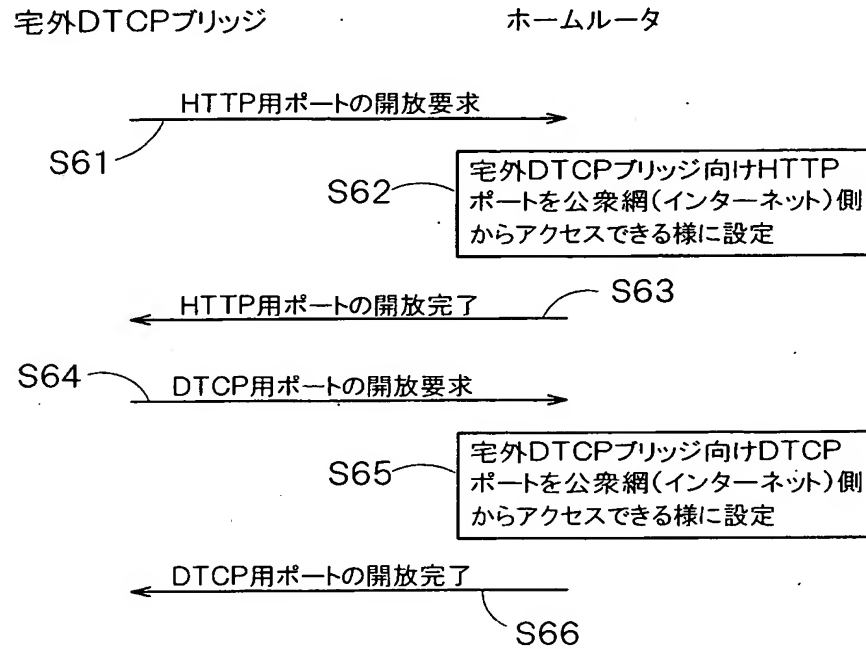


【図9】

宅外DTCPブリッジの内部構成(第2の実施例)



【図10】

第2の実施形態の宅外DTCPブリッジとホームルータ間のシーケンス

【書類名】 要約書

【要約】

【課題】 宅内ネットワーク間で送受信される情報を、著作権保護を図りつつ、宅外ネットワーク間でも送受信を行う。

【解決手段】 本発明に係る通信システムは、ユーザ宅 1 内に設置された送信装置 2、ホームネットワーク 3 及び宅外 DTCP ブリッジ 4 と、ユーザ宅 1 にインターネット 5 を介して接続される宅外の受信装置 6 とを備えている。宅外 DTCP ブリッジ 4 は、宅内ネットワーク I/F 部 11 と、DTCP 関連パケットフィルタ 12, 13 と、DTCP 処理部 14 と、ホームルータ及びファイアウォール部 15 と、宅外ネットワーク I/F 部 16 とを有する。ユーザ宅 1 内の宅外 DTCP ブリッジ 4 に宅外デバイス登録テーブル 25 を設け、このテーブルに予め登録された受信装置 6 のみにユーザ宅 1 内からのコンテンツ送信を許可するため、著作権保護を図る必要のあるコンテンツの不正コピーや不正取得を防止しつつ、正規のユーザに対して宅外でもコンテンツを利用できる機会を与えることができる。

【選択図】 図 2

特願 2002-344431

出願人履歴情報

識別番号

[000003078]

1. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
 住 所 東京都港区芝浦一丁目1番1号
 氏 名 株式会社東芝

2. 変更年月日 2003年 5月 9日
[変更理由] 名称変更
 住所変更
 住 所 東京都港区芝浦一丁目1番1号
 氏 名 株式会社東芝